IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 12, December 2017

Securing Text and Video by Using Text Hiding Technique and 4-Level Discrete Wavelet Domain and SVD Techniques with Error Correcting Coding

Gagan Kumar Dewangan [1], Mr. Suman Swarnkar [2], Mr. Ghanshyam Sahu [3]

B.C.E.T., Durg, C.G. India [1]

Professor, B.C.E.T., Durg, C.G. India [2]

Assistant Professor, B.C.E.T., Durg, C.G India [3]

Abstract: The rapid expansion of the Internet in the past years has immediately increased the availability of digital data such as audio, images and videos to the general public. Whilst the computers are more and more incorporated via the system, the supply of digital press has gotten faster, easier, and also requiring less attempt to make accurate copies. One of the key impediments will be the dearth of strong intellectual property security of digital networking to discourage unauthorized copying and supply. In this paper, a powerful technique to protect text and video is suggested which makes use of text hiding technique and watermarking algorithm based on Discrete Wavelet Transform (DWT), Singular value decomposition and Hamming error code to procuring video and text. Initially measure the writing will be hidden in the image using LSB algorithm then in second measure frames will be pulled and watermarking is used on singular worth subsequent to the SVD is completed. Before renewing added parity bits are inserted to create the watermarking method more secure and powerful. Preliminary results reveal that this suggested technique is robust to the previous signal processing techniques and geometric distortions.

Keywords: Steganography, LSB Algorithm, Digital watermark, Discrete Wavelet Transform, Singular Value Decomposition (SVD), Video Watermarking, Hamming Code.

I. INTRODUCTION

Digital watermarking technology is an emerging field of computer Engineering, cryptography, signal processing and communications. Digital watermarking is supposed by its developers as the solution to the need to offer value added security on top of data security and scrambling for content protection. In general a digital watermark is a technique which enables somebody to add hidden copyright information or other confirmation message into digital networking. Watermarking is the procedure which implements data known as a watermark or digital signature or label or label into a multimedia thing like that watermark can be detected or extracted later to generate an assertion regarding the item. Digital watermark can be a sequence of information comprising the owners copyright for the multimedia data. It's inserted visibly or invisibly into another image so that it could be extracted later being a proof of owner. Usage of electronic image watermarking technique has grown considerably to safeguard the copyright ownership of digital multimedia data because it is very much prone to unlawful and unauthorized replication, reproduction and manipulation. The watermark could be a symbol, label or an arbitrary sequence. A typical excellent watermarking scheme should aim at keeping the embedded watermark very robust under malicious attack in real and midsize domain. Incorporation of the watermark from the image could possibly be performed in various ways.

Text procuring is completed using steganography technique that's the science and art of hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused data in ordinary computer files (such as pictures, sound, text, HTML, or even floppy disks) with bits of different, invisible data. This hidden information can be plain text, cipher text, text or even graphics. Steganography sometimes is used when encryption isn't permitted. Or, more commonly, steganography can be utilized to nutritional supplements collateral. A encrypted document might hide information using steganography, therefore even though the encoded file is flashed, the hidden message is not seen.

II. RELATED WORK

Video watermarking is also well called the procedure for embedding copyright data in video piece streams [1]. It was proposed in the past several years to fix the dilemma of illegal misuse and distribution of digital video. Within this study, an effective, robust and undetectable movie watermarking algorithm has been suggested for copyright protection.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 12, December 2017

This algorithm was based on a cascade of two powerful mathematical alterations; Discrete Wavelets Transform (DWT) and Singular Value Decomposition (SVD). Two different alter domain methods demonstrated higher level of distinct and distinct quantities of robustness against precisely the exact same attack will be achieved by using their own combination. In another work, a novel wavelet-based multiresolution digital watermarking system for color graphics James [two] is discussed. The algorithm in Wave Mark uses discrete wavelet transforms and error-correcting coding approaches to present robust watermarking of digital graphics. Unlike other wavelet-based algorithms, our watermark retrieval procedure does not expect a match with an uncorrupted original image. The plan uses Daubechies' advanced level wavelets and extended Hamming codes to deal with problems associated with JPEG compression and random additive noise. Within this paper, a successful watermarking scheme based on Radon transform for landscape picture is used [3]. The robustness against turning attack is achieved using the translation property of the Radon transform. The Radon transform emphasizes and finds the linear characteristic to calculate the angle of image spinning. The watermark can be a hologram generated by quantization depending on the cover image. The procedure used hologram quantization to disperse the watermark information and analyse the cover image thickness. The hologram is transformed by a discrete fractional random change (DFRNT) with a random seed β. This makes the watermark security. The planned procedure uses different wavelet transform (DWT) domain names. DWT domain watermarking is powerful to indicate processing attacks. For improving the accuracy of detecting, we adjust the guts of detachable and image which the pixels of image boundary move 1 notch at one time. The algorithm can be robust to the adrenal Impact attack. Video watermarking is also well-known as the process of encrypting copyright information in video piece streams [4]. It had been proposed in the last several years to take care of the issue of illegal manipulation and supply of video. In this study, an effective, powerful and undetectable movie watermarking algorithm was proposed for copyright security. This algorithm was based on a cascade of 2 powerful mathematical transforms; Discrete Wavelets Transform (DWT) and Singular Value Decomposition (SVD). Two different alter domain techniques revealed elevated amount of distinct and unique degrees of robustness against precisely the exact same attack will be achieved through their own combination.

III.PROBLEM IDENTIFICATION

Watermarking is a potential method to discourage unauthorized copying or attest the source of the image. Broadly speaking, digit watermarks must meet the following requirements.

- Imperceptible: The watermark should be undetectable to human watch whilst the server image is embedded with confidential data and prohibited removal of watermark must not be possible.
- Secure and reliable: The embedded watermark cannot be deleted and retrieved by the host image, even if the embedded algorithms are understood.
- Robust: The watermarked image must be resistant encounter almost any geometric and signal distortion processing. The watermark can survive from each of the international attacks like as JPEG compression, resizing and cropping.
- Unambiguous: The objective of watermarking technique incorporates author identification, affirmation, and copyright protection. The watermark logo has to be siphoned identifying the proprietor

The present limitations confronted in the Field of Video watermarking are as follows:

- Digital watermarking algorithms usually use the lower-order bit-planes of their first image, therefore do deliberate disturbance calculations.
- Can't be added to downgrade the quality of the source image a lot of.
- Digital watermark subscribers are often widely accessible.
- There's a limited amount of data that can be used to fit digital water marks in an extremely compressed JPEG image.
- Noticeable artifacts of picture Compression usually ruin watermarks easily.

IV.PROPOSED METHODOLOGY

A. Discrete Wavelet Transform

Wavelet transform is a Moment Domain localized analysis method with the windows size fixed and forms convertible. There is quite great time differentiated speed in frequency part of signals DWT transformed. Additionally there's quite great frequency distinguished speed in its own low frequency part. It can distill the information from signal efficiently. The basic idea of discrete wavelet transform (DWT) in image procedure is to multi-differentiated decompose the image into sub-image of different plasma domain and independent frequency district. Then transform the coefficient of all sub-images. Subsequent to the original image has been DWT altered, it's decomposed into 4 frequency districts which is 1 low-frequency district(LL) and also three high-income districts(LH,HL,HH).

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 12, December 2017

B. Singular Value Decomposition

The Singular Value Decomposition (SVD) is a method that can be used in Image compression methods, but could be applied to watermarking. The SVD is performed, after that the singular values usually are modified to embed the watermark. A pseudo-inverse SVD is then employed to acquire the original content. The SVD can be used on its own for watermarking, but is also frequently used in hybrid methods such in which combines the SVD and the discrete cosine transform. The SVD is relatively computationally complex, but by applying it into hybrid vehicle techniques it might not be essential to do an SVD on the entire picture, reducing the computational complexity.

C. Hamming Code

The most common Kinds of error-correcting codes used in RAM are based on The codes invented by R. W. Hamming. From the Hamming code, k parity bits are inserted to an n-bit statistics sentence, forming a new word of +k bits. The bit positions are numbered in sequence from 1 to n + k. Those positions numbered with forces of two are earmarked for the parity bits. The remaining pieces are the data pieces. The code is applied in combination with words of almost any period.

D. LSB (Least Significant Bit) Algorithm for hiding text from image

An electronic picture is described with a 2 D matrix of these colour intestines At each grid point (i.e. pixel). Normally grey images utilize 8 bits, whereas colored uses 2-4 pieces to describe the color model, for example as for example RGB model. The Steganography system which uses an image as the pay, there are lots of methods to hide information inside cover-image. The spatial domain methods manipulate the cover-image pixel piece values to embed the secret details. The secret pieces are written straight to the cover image pixel bytes. Consequently, the spatial domain methods are easy and simple to implement. The Least Significant Bit (LSB) is one of the principal methods in spatial domain image Steganography. The LSB will be your smallest significant bit at the byte importance of the image pixel. The LSB cantered image steganography embeds the secret at least significant bits of pixel values of this pay image (CVR).

The concept of LSB Embedding is simple. It exploits the fact that the Amount of accuracy in most image formats is much greater than that perceivable By ordinary human vision. Consequently, a modified picture with Small variations in Its colours will probably be equal from the original by an individual being, only By studying it. In conventional LSB technique, which requires eight bytes of Pixels to store 1byte of secret data also in proposed LSB technique, only four Bytes of pixels are sufficient to put on one message byte. Remainder of the bits in The pixels remains the same.

E. *Proposed Algorithm*

The basic steps involved in DWT based watermarking algorithm are as follows:

1. Hide text in Image to be used for watermarking using LSB hiding technique which is as given below:
    a. Read the secret and cover image and convert them into gray scale images,
    b. Check the size of the secret image with that of the cover image such that size of the secret image should be less than cover image.
    c. Encode the secret image into binary using bit gate command and divide it into RGB parts.
    d. Substitute MSB bits of secret image into LSB bits of cover image. Hide the password with Stego image.
    e. The reverse process takes place at the receiving end.
2. Divide the video clip into video frames.
3. Convert every video frame F from RGB to YUV colour matrix format.
    a. Y = 0.2989 * R + 0.5866 * G + 0.1145 * B
    b. U= -0.1687*R-0.3312*G+0.5*B
    c. V = 0.5 * R - 0.4183 * G - 0.0816 * B
4. Apply 4 levels DWT algorithm. Separate the frame into a lower resolution approximation image (LL) as well horizontal (HL), vertical (LH) and diagonal (HH).
5. The LL band stands for the coarse one which represents the low frequency part where most energy focuses.
6. The sub-bands labelled HL, LH, and HH represent the details of wavelet coefficients.
7. To obtain the next coarser wavelet coefficients, the sub band LL is further decomposed as shown in Figure 1.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 12, December 2017

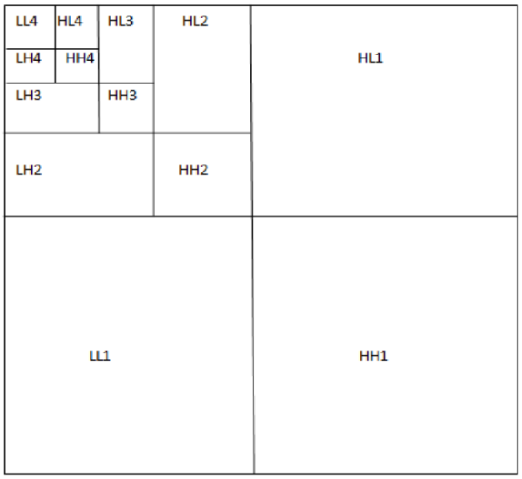

Figure 1: 4-Level Wavelet DWT decomposition

1. The basic steps involved in proposed algorithm are as follows:
2. Convert the video frame into an m x n matrix let it be A, by decomposition of the matrix A we get A= USV where U is an m x n orthogonal matrix and V is an n x n orthogonal matrix. S is a diagonal matrix such that S = diagonal (s1 , s2, s3 , ..., sk , 0, 0, ..0) where si's are the singular values of A and are in descending order.
3. Apply the SVD operator on the mHL4 sub-band. The SVD operator decomposes the sub-band's coefficient matrix into three independent matrices: mHL4 = UwHL4 SwHL4 VwHL4.
4. A Hamming code is used to add redundancy to the bits so that the errors can be detected or corrected to a certain extent. Hamming code is a linear block code. The main advantage of linear block codes is their simplicity in implementation and low computational complexity.
    a. In the Hamming code, k parity bits are added to an n-bit data word frame, forming a new word of n +k bits. The frame bands are converted to binary. The hamming code is added to binary bits.
    b. The bit positions are numbered in sequence from 1 to n + k. Those positions numbered with powers of two are reserved for the parity bits.
    c. The remaining bits are the data bits. The code can be used with words of any length.
5. Embed the watermark bits into LSB (Least Significant Bit) into LSB bit of SHL4.
6. The watermark extraction procedure will be the reverse of the above process.

Bit position	1	2	3	4	5	6	7	8	9	10	11	12
	P_1	P_2	1	P_4	1	0	0	P_8	0	1	0	0

Figure 2: Hamming code example

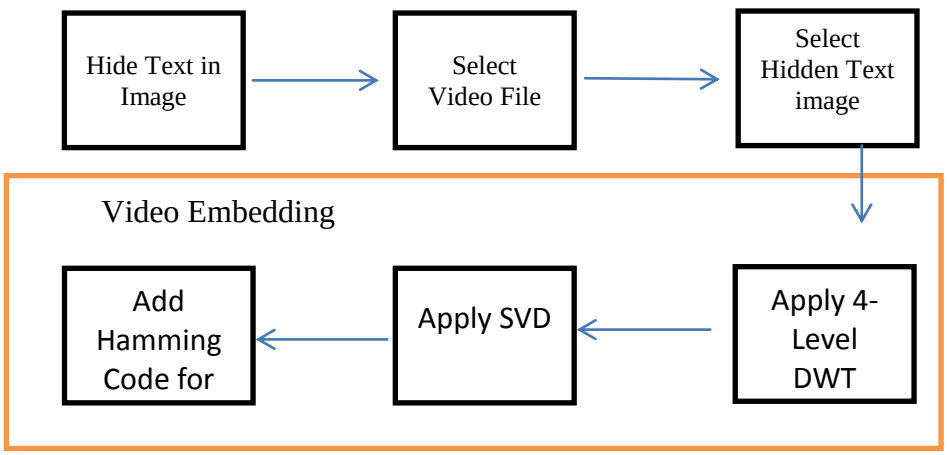

Figure 3: Block diagram of Watermark Embedding

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 12, December 2017

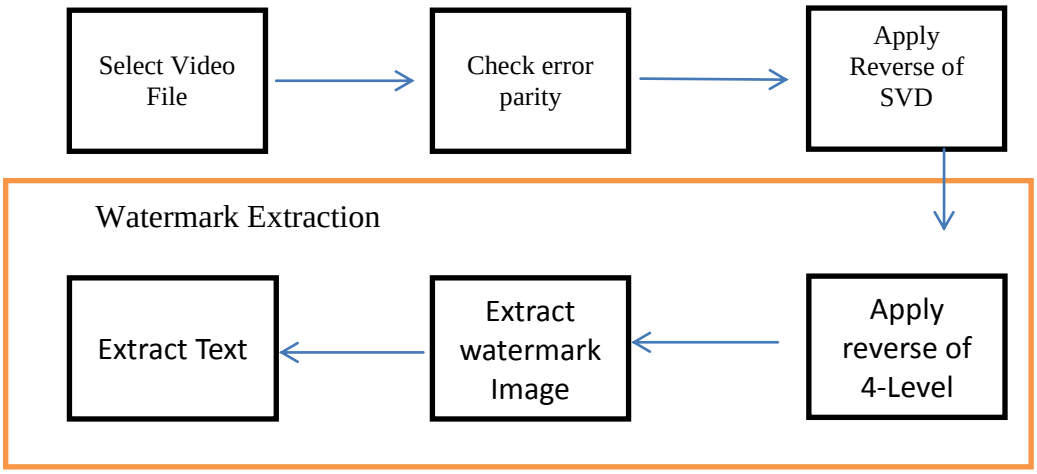

Figure 4: Block diagram of Watermark Extraction

V. EXPERIMENTAL RESULTS

The proposed work was implemented using Matlab software. The text is first hidden in the watermarked image and the same image is used for watermarking. A grey scale watermarked image has been used embedding. The performance of the proposed watermarking scheme was measured using the several video formats . The size of the watermarking image was 256 * 198. It used Hamming error detection method to add parity bits.

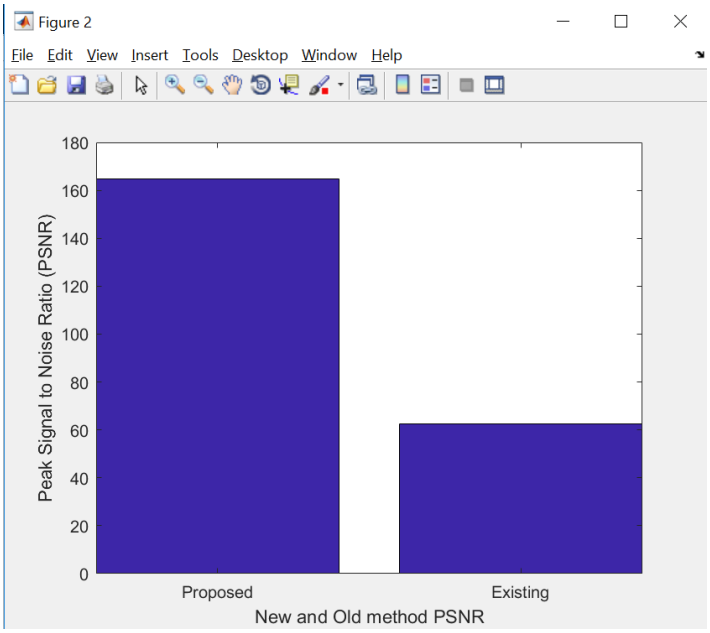

Figure 5: PSNR value of Proposed and Existing method

The watermark's invisibility is generally measured using the peak signal-to-noise ratio (PSNR) which is most commonly used to measure the quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. The equation for calculating PSNR value is as follows:

$$\text{PSNR} = 20log_{10}(\frac{255}{MSE}) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

The figure 5 shows that the proposed method PSNR value is much greater than that of existing method.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 12, December 2017

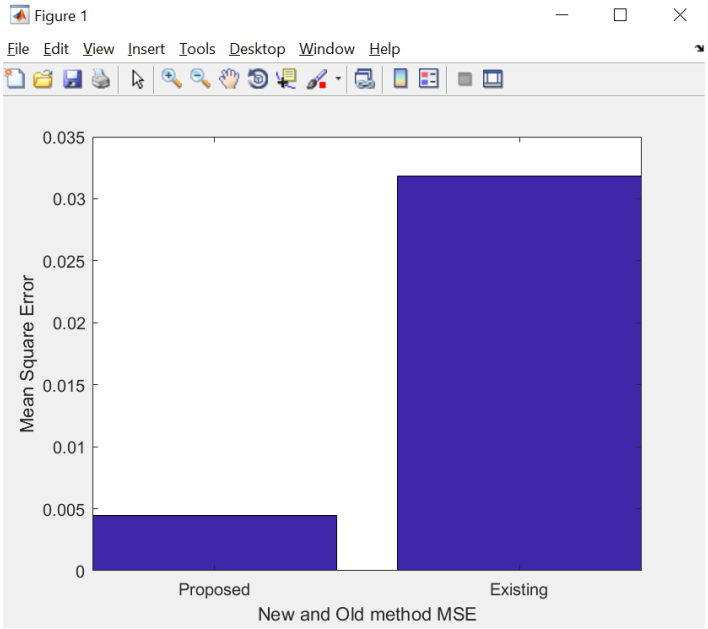

Figure 6: MSE value of Proposed and Existing method

The MSE represents the cumulative squared error between the compressed and the original image.

$$\text{MSE} = \sqrt{\frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{M}[f^{\omega}(x,y) - f(x,y)]} \quad ^{2} \ldots\ldots\ldots\ldots\ldots (5)$$

The figure 6 shows that the proposed method MSE value is much small than that of existing method. The figure 5 shows that the proposed method MSE value is much greater than that of existing method.

File name	PSNR value		MSE value	
	Proposed	Existing	Proposed	Existing
Video1.avi	164.7237	62.92	0.80793	0.93338
Video2.mpg	167.9673	152.69	0.12337	0.00126
Video3.avi	167.1515	150.91	0.62874	0.4444
Video4.avi	167.6008	160.51	0.27488	0.034
Video5.avi	168.0188	100.11	0.95389	0.5535
Average PSNR and MSE	167.09242	125.428	0.5577662	0.393308

Table 1 PSNR and MSE values for different video formats

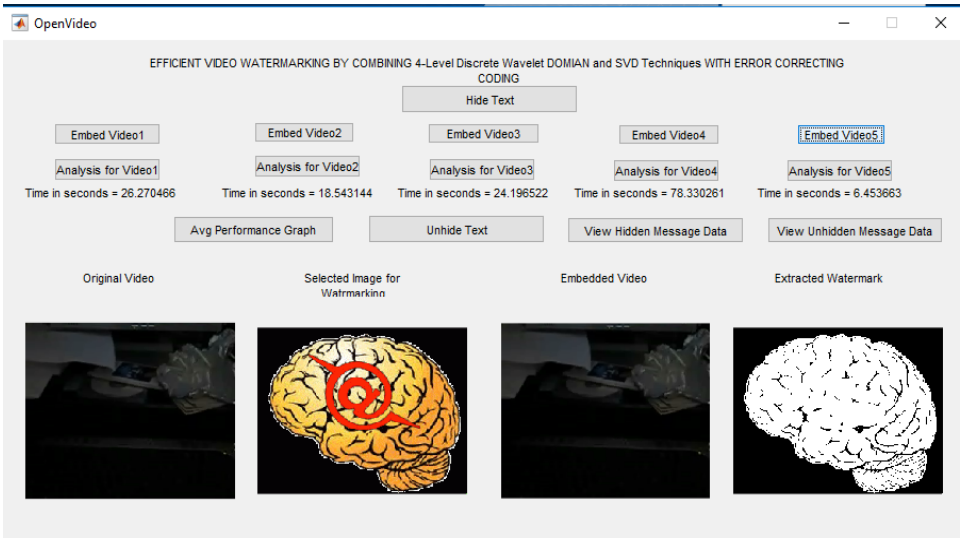

Figure 7: The screenshot of proposed method

DOI 10.17148/IJARCCE.2017.61221

Figure 7 shows the proposed work screen the user first hides text by using hide text option. The embedding can be performed by using embed video options. After extraction of watermarked image the text is extracted from image using unhide text options.

VI. CONCLUSION

The task within video watermarking would be always to improve the tradeoff between about three measurements of watermarking specifically imperceptibility, robustness and payload. The suggested digital video watermarking strategies really are a little contribution for the area of electronic video watermarking. Inside this informative article, target is really on evolution of movie watermarking schemes which can be undetectable, stable, and powerful. The proposed strategy employs the methods for DWT, SVD and also Hamming procedure set for watermarking video and text at a safe and successful method. In future there is a scope for increasing the utility of the proposed scheme for varying degrees of compression.

REFERENCES

[1] Shafali Banyal and Shivi Sharma, " Digital Video Watermarking Using DWT and SVD Techniques", IJARCCE,2016.
[2] Padmini K and Champakamala B S,"Image Hiding using Least Significant Bit Algorithm Steganography", Proc. of Int. Conf. on Current Trends in Eng., Science and Technology, ICCTEST,2017.
[3] James Ze Wang and Gio Wiederhold, "WaveMark: Digital Image Watermarking
[4] Using Daubechies' Wavelets and Error Correcting Coding", Stanford University,1995.
[5] Vinicius Licks and Ramiro Jordan, "Geometric Attacks on Image Watermarking Systems," IEEE Signal Processing Magazine, vol. , 2016.
[6] Ruichen Jin and Jongweon Kim" A Robust Watermarking Scheme for City Image," International Journal of Security and Its Applications, 2016.
[7] Nazia Azeem , Iftikhar Ahmad , Syed Roohullah Jan , Muhammad Tahir , Farman Ullah and Fazlullah Khan , " A New Robust Video Watermarking Technique Using H.264/AAC Codec Luma Components Based On DCT", *IJARIIE*, 2016.
[8] Rini T Paul, " Video Watermarking Based On DWT-SVD Techniques," International Journal of Science and Research (IJSR), 2014.
[9] Vandana Yadav , Dr. Parvinder Singh and Jasvinder Kaur, " DWT-SVD Based Digital Image Watermarking Using GA," International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 7, July 2015 .
[10] Baoru Han and Jingbing Li, "Watermarking algorithm for medical volume data anti-geometric attacks", *Biomedical Research 2016*.
[11] Yonghong Chen and Jiancong Chen, " Digital Image Watermarking Based on Mixed Error Correcting Code," *Journal of Information Security*, 2012 .
[12] Bhaskaran et al.," Fragile Watermark for Detecting Tampering in images", U. S. Patent Number 6064764, may 16,2000.
[13] H.-Y. Huang, C.-H. Yang, and W.-H. Hsu, "A video watermarking technique based on pseudo-3-D DCT and quantization index modulation," IEEE Trans Inf. Forensics Security, vol. 5, no. 4, pp. 625–637, Dec. 2010.
[14] Maneli Noorkami, and Russell M. Mersereau," Digital Video Watermarking in P-Frames With Controlled Video Bit-Rate Increase", IEEE Transactions on Information Forensics and Security, VOL. 3, NO. 3, SEPTEMBER 2008.
[15] Jordi Serra-Ruiz and David Megias, "DWT and TSVQ-based semifragile watermarking scheme for tampering detection in remote sensing images," 2010 Fourth Pacific-Rim Symposium on Image and Video Technology.
[16] J. Zhang, A. T. S. Ho, G. Qiu, and P. Marziliano, "Roubust video watermarking of H.264/AVC," IEEE Trans. Circuits Syst., vol. 54, no. 2, pp. 205–209, Feb. 2007. [16]. Y. Wang and A. Pearmain," Blind MPEG-2 video watermarking in DCT domainrobust against scaling," IEE Proc.-Vis. Image Signal Process., Vol. 153, No. 5, October 2006.
[17] P. Chan and M. Lyu, "A DWT-Based Digital Video Watermarking Scheme with Error Correcting Code," in Proceedings of the 5th International Conference on Information and Communications Security, 2003, pp. 202- 213.
[18] X. Niu and S. Sun, "A New Wavelet-Based Digital Watermarking for Video," in Proceedings of the 9th IEEE Digital Signal Processing Workshop, 2000, pp. 241-245. [19] S. Voloshynovskiy, S. Pereira, and T. Pun, "Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks," Comm. Magazine, vol., pp. 118-126, Aug. 2001.
[19] E. Ganic and A. M. Eskicioglu, "Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," ACM Multimedia and Security Workshop 2004, Magdeburg, Germany, September 20-21, 2004.
[20] J. Lee et al, A survey of watermarking techniques applied to multimedia, IEEE International Symposium on Industrial Electronics, Vol. 1, pp. 272-277, 2001.
[21] Ankita A. Hood "A Review on Video Watermarking and Its Robust Techniques" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 1, Januaryr- 2013 ISSN: 2278- 0181, page no.1-6
[22] Amit Singh, Susheel Jain, Anurag Jain "A Survay: Digital Video Watermarking" International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013 ISSN 2229-5518 page no. 1261- 1265
[23] Farooq Husain"A Survey of Digital Vatermarking Techniques for multimedia data", MIT International Journal of Electronics and communication Engineering, Vol 2, No.1, Jan 2012 PP. (37-43) ISSN 2230-7672
[24] Harleen Kaur "Study on Audio and Video Watermarking", International Journal of Communication Network Security ISSN: 2231 – 1882, Volume-2, Issue-1, 2013, PP-34-38.